Advances in Mathematics of Communications
Volume 14, No. 4, 2020, 573–577

doi:10.3934/amc.2020030

GIOPHANTUS DISTINGUISHING ATTACK IS A LOW DIMENSIONAL LEARNING WITH ERRORS PROBLEM

Jintai Ding

University of Cincinnati
Cincinnati, OH 45219, USA

Joshua Deaton and Kurt Schmidt*

University of Cincinnati
Cincinnati, OH 45219, USA

(Communicated by Lih-Chung Wang)

Abstract. In this paper, we attack the recent NIST submission Giophantus, a public key encryption scheme. We find that the complicated structure of Giophantus's ciphertexts leaks information via a correspondence from a low dimensional lattice. This allows us to distinguish encrypted data from random data by the LLL algorithm. This is a more efficient attack than previous proposed attacks.

1. Introduction

In November, 2017 Koichiro Akiyama *et al* proposed Giophantus, a "new" public-key encryption scheme based on non-linear indeterminate equations. In the proposal Akiyama *et al* made what they called the Indeterminate Equations Learning with Errors (IE-LWE) assumption which is an extension of the Ring Learning with Errors assumption [1] which is in turn based on the shortest vector problem of a lattice. IE-LWE loosely states that, given a fixed public key of Giophantus, it is "impossible" to distinguish encrypted data from uniform random data. The authors showed that under IE-LWE Giophantus is provably secure in the sense of indistinguishability under chosen plaintext attack (IND-CPA) [1]. That is, if an adversary chooses two messages of equal length, and Giophantus randomly encrypts one, the adversary can not achieve better than fifty percent probability to correctly guess which of the messages was encrypted.

However, attacks against Giophantus were discovered showing IE-LWE is false, though these attacks ignore Giophantus's lattice structure causing inefficiency. On January 11th, 2018 on the NIST Comments Section, Wouter Castryck and Frederik Vercauteren falsely claimed they could break Giophantus's IND-CPA security [4]. On April 12th, 2018, Akiyama disputed Castryck's and Vercauteren's attack [2]. Most recently, on June 11th, 2018, Ward Beullens *et al* revised the January 11th attack and claimed that there exists a non-negligible distinguishing advantage [4], where the distinguishing advantage is defined to be twice the probability of a correct guess minus one. Beullen's attack uses statistical analysis on the ciphertext to

2020 *Mathematics Subject Classification:* Primary: 94A60, 68P25; Secondary: 81P94.

Key words and phrases: Lattice, post quantum cryptography, learning with errors, Giophantus, cryptanalysis, NIST..

J. Ding and K. Schmidt are partially supported by US Air Force.

* Corresponding author: Kurt Schmidt.

achieve such an advantage. Further, we confirmed by private communication with Akiyama that, using the same statistical analysis on the ciphertext, an attack was developed so that if given around ten million samples one can distinguish whether they are encrypted data or random data.

The intuition from the work of Ding [5] and Fluhrer [6] gives us a strong hint that the design of this system leaks information due to its complicated structure. This lead us to a new attack on ciphertexts that uses a lattice reduction instead of statistical analysis that provides a stronger result. Namely, given one sample, we are able to distinguish whether it is encrypted data or random data. We will first recall the Giophantus encryption scheme then introduce our attack on Giophantus.

2. Giophantus

We begin by recalling the parameters of Giophantus. The primary parameters are two prime numbers n and q. Specifically, Akiyama gives n and q, where q is the next prime after $324n^2 + 72n + 15$, for the following NIST security categories (Category, n) : (I, 1201), (III, 1733), and (V, 2267) [2].

We start with a field F_q of size q. Next we construct the quotient ring $R_q = F_q[t]/(t^n - 1)$ and R_4, a subset of R_q, whose polynomials coefficients are in the range of $\{0, 1, 2, 3\}$. The public key $X(x, y)$ is an irreducible bivariate polynomial over R_q where $X(x, y) = 0$ has a solution $u_x(t), u_y(t) \in R_4$. The secret key is the solution $u_x(t), u_y(t)$. In practice the degree of $X(x, y)$ is 1. To encrypt a message $m(t) \in R_4$ we generate random polynomials $r(x, y)$ over R_q and $e(x, y)$ over R_4. In practice the degree of $r(x, y)$ is 1, while the degree of $e(x, y)$ is 2. Then we calculate the ciphertext $c(x, y) = X(x, y)r(x, y) + 4e(x, y) + m(t)$. To decrypt, first we plug $u_x(t), u_y(t)$ into $c(x, y)$ and find $c(u_x(t), u_y(t)) = m(t) + 4e(u_x(t), u_y(t))$. Finally, q was chosen large enough to ensure that each coefficient of $c(u_x(t), u_y(t))$ is smaller than q. So, we recover $m(t)$ by modding each coefficient of $c(u_x(t), u_y(t))$ by 4.

For the rest of the paper we write $X(x, y), r(x, y), e(x, y)$ as:

- $X(x, y) = a_{10}(t)x + a_{01}(t)y + a_{00}(t)$
- $r(x, y) = r_{10}(t)x + r_{01}(t)y + r_{00}(t)$
- $e(x, y) = e_{20}(t)x^2 + e_{11}(t)xy + e_{02}(t)y^2 + e_{10}(t)x + e_{01}(t)y + e_{00}(t)$

where $a_{i,j}(t), r_{i,j}(t) \in R_q$ and $e_{i,j} \in R_4$ (the index of the coefficient corresponds to degree of x and y, respectively).

3. Our attack

All attacks against Giophantus use the ring homomorphism between R_q and F_q given by evaluating $f(t) \in R_q$ at $t = 1$. Throughout the remainder of the paper for any polynomial $f(t) \in R_q$ we denote $f(1)$ as f'.

We are able to distinguish ciphertexts from degree 2 polynomials sampled uniformly from $R_q[x, y]$. More precisely given a public key $X(x, y)$, if we denote the set of ciphertexts as $\mathcal{C} =$

$$\{X(x,y)r(x,y)+4e(x,y)+m(t) : r(x,y) \in R_q[x,y]\ ,\ e(x,y) \in R_4[x,y]\ ,\ m(t) \in R_4\}$$

and an oracle uniformly chooses a polynomial $g(x, y)$ from $\mathcal{C}$ or $R_q[x, y]$, we are able to correctly identify whether $g(x, y) \in R[x, y] \setminus \mathcal{C}$ or not.

Our attack is to transform a ciphertext into a low-dimensional Learning with Errors (LWE) problem. Thus, reformulating the problem of distinguishing between encrypted data from random data into a low-dimensional decision version of LWE.

We give a brief, informal description of the decision version of LWE. Given that p is prime, A is a $m \times n$ matrix over $\mathbb{Z}_p$, and χ is an error distribution on $\mathbb{Z}_p$ that strongly favors "small" elements of $\mathbb{Z}_p$. The decision version of LWE is to distinguish between the uniform distribution on $\mathbb{Z}_p^{m\times n} \times \mathbb{Z}_p^m$ and the distribution $(A, b = As + e)$ where s is sampled uniformly at random from $\mathbb{Z}_p^n$ and $e \leftarrow \mathbb{Z}_p^m$ according to χ. For a more precise definition see [8].

To start we expand the ciphertext $c(x, y) = X(x, y)r(x, y) + 4e(x, y) + m(t)$ and evaluate each coefficient at $t = 1$. We obtain, $c'(x, y) = f'_{20}x^2 + f'_{11}xy + f'_{02}y^2 + f'_{10}x + f'_{01}y + f'_{00}$. Where

$$\begin{aligned}
f'_{20} &= a'_{10}r'_{10} + 4e'_{20}\\
f'_{11} &= a'_{10}r'_{01} + a'_{01}r'_{10} + 4e'_{11}\\
f'_{10} &= a'_{10}r'_{00} + a'_{00}r'_{10} + 4e'_{10}\\
f'_{20} &= a'_{01}r'_{01} + 4e'_{02}\\
f'_{01} &= a'_{01}r'_{00} + a'_{00}r'_{01} + 4e'_{01}\\
f'_{00} &= a'_{00}r'_{00} + 4e'_{00} + m'
\end{aligned}$$

Notice we can express the above system as,

$$\begin{bmatrix} f'_{20}\\ f'_{11}\\ f'_{10}\\ f'_{02}\\ f'_{01}\\ f'_{00}\end{bmatrix} = \begin{bmatrix} a'_{10} & 0 & 0\\ a'_{01} & a'_{10} & 0\\ a'_{00} & 0 & a'_{10}\\ 0 & a'_{01} & 0\\ 0 & a'_{00} & a'_{01}\\ 0 & 0 & a'_{00}\end{bmatrix} \begin{bmatrix} r'_{10}\\ r'_{01}\\ r'_{00}\end{bmatrix} + \begin{bmatrix} 4e'_{20}\\ 4e'_{11}\\ 4e'_{10}\\ 4e'_{02}\\ 4e'_{01}\\ 4e'_{00} + m'\end{bmatrix} \tag{1}$$

In order to view this as a LWE problem, we must reduce the size of the right most vector. To do this we use Phong Nguyen's idea of subtracting the expected value, which he described in the NIST Comments Section [7]. Since n is sufficiently large, according to the central limit theorem, for any $g(t) \in R_4$, g' will approximately follow a truncated discrete Gaussian distribution [4]. To calculate the expected value of g' we multiply the expected value of a coefficient of $f(t)$ by n. So we find the expected value of g' is $n \cdot \frac{0+1+2+3}{4} = \frac{3n}{2}$. This shows that the expected value of $4g'$ equals $6n$. Since $m(t) \in R_4$, the closest integer to the expected value of $4g' + m'$ equals $\lceil \frac{15n}{2} \rceil$. To calculate the variance, we find the variance of a coefficient of $g(t)$ and multiply by n. So, the variance is $n(\frac{0+1+4+9}{4} - \frac{9}{4}) = \frac{5n}{4}$. Hence the variance of $4g(t)$ is $20n$, and the variance of $4g(t) + m(t)$ is $\frac{85n}{4}$.

Now if we subtract $\begin{bmatrix} 6n & 6n & 6n & 6n & 6n & \lceil \frac{15n}{2} \rceil \end{bmatrix}^T$ from (1) we obtain

$$\begin{bmatrix} \tilde{f}'_{20}\\ \tilde{f}'_{11}\\ \tilde{f}'_{10}\\ \tilde{f}'_{02}\\ \tilde{f}'_{01}\\ \tilde{f}'_{00}\end{bmatrix} = \begin{bmatrix} a'_{10} & 0 & 0\\ a'_{01} & a'_{10} & 0\\ a'_{00} & 0 & a'_{10}\\ 0 & a'_{01} & 0\\ 0 & a'_{00} & a'_{01}\\ 0 & 0 & a'_{00}\end{bmatrix} \begin{bmatrix} r'_{10}\\ r'_{01}\\ r'_{00}\end{bmatrix} + \begin{bmatrix} \tilde{e}'_{20}\\ \tilde{e}'_{11}\\ \tilde{e}'_{10}\\ \tilde{e}'_{02}\\ \tilde{e}'_{01}\\ \alpha\end{bmatrix}$$

where for each pair ij excluding 00, $\tilde{f}'_{ij} = f'_{ij} - 6n$, $\tilde{f}'_{00} = f'_{00} - \lceil \frac{15n}{2} \rceil$, $\tilde{e}'_{ij} = 4e'_{ij} - 6n$ and $\alpha = 4e'_{00} + m' - \lceil \frac{15n}{2} \rceil$. If we denote $\vec{f}$, A, $\vec{r}$, $\vec{e}$ accordingly then, $\vec{f} = A\vec{r} + \vec{e}$ is a LWE problem, where $\vec{r}$ is the secret vector and $\vec{e}$ is the noise vector. Further, the first five components of $\vec{e}$ approximately follow a truncated discrete Gaussian distribution over $\{-6n,\dots,6n\}$ with $\sigma^2 = 20n$ while the sixth component of $\vec{e}$ is over $\{-\lceil\frac{15n}{2}\rceil,\dots,\lfloor\frac{15n}{2}\rfloor\}$ with $\sigma^2 = \frac{85n}{4}$. Though this slightly deviates from the LWE definition, experimental evidence indicates that this does not impact the shortest vector in the lattice.

Next we use a lattice reduction attack to solve the LWE problem that Albrecht outlined in [3]. Consider the row space of A^T, where scalar multiplication is from $\mathbb{Z}_q$. We want a lattice, $\Lambda \subseteq \mathbb{Z}^6$, where every element of the row space of A^T also belongs to Λ when each component is viewed as an integer and every element of Λ also belongs to the row space of A^T when each component is modded by q. To find a basis for Λ we first compute the row reduce echelon form of A^T and view it over the integers. So, if $\mathrm{RREF}(A^T) = \begin{bmatrix} I_3 & \bar{A}\end{bmatrix}$ then we view both $I_3 \in \mathbb{Z}^{3\times 3}$ and $\bar{A} \in \mathbb{Z}^{3\times 3}$. Next, we undo the modular reductions by padding $\mathrm{RREF}(A^T)$ with multiplies of q. More precisely, we stack $\begin{bmatrix} I_3 & \bar{A}\end{bmatrix}$ on top of $[0_{3\times 3}\ qI_3]$. We get a basis B of Λ where

$$B = \begin{bmatrix} I_3 & \bar{A} \\ 0_{3\times 3} & qI_3 \end{bmatrix} \in \mathbb{Z}^{6\times 6}.$$

We say that $\Lambda(B_{c'(x,y)})$ is the lattice that corresponds to $c'(x,y)$. Now that we have basis for Λ, we look for the closest vector in Λ to $\vec{f}^{\,T}$ (viewed over the integers). Since $\vec{r}^{\,T}A^T - \vec{f}^{\,T} = -\vec{e}^{\,T}$ and the e'_{ij}'s are small, we suspect the closest vector in Λ to $\vec{f}^{\,T}$ is $\vec{s}^{\,T}A^T$.

We extend our basis B to include our target. Our extended basis, $\bar{B}_{c'(x,y)}$ is

$$\bar{B}_{c'(x,y)} = \begin{bmatrix} I_3 & \bar{A} & 0 \\ 0_{3\times 3} & qI_3 & 0 \\ \multicolumn{2}{c}{\vec{f}^{\,T}} & 1 \end{bmatrix}$$

Now, we know that $[\vec{e}^{\,T}|1] \in \Lambda(\bar{B})$ because $[-\vec{x}|1]\bar{B}_{c'(x,y)} = [\vec{e}^{\,T}|1]$.

Further, we know there is a high probability that $[\vec{e}^{\,T}|1]$ is the shortest vector in $\Lambda(\bar{B}_{c'(x,y)})$ as the e'_{ij}'s are small. To recover $\vec{e}^{\,T}$ we perform a lattice reduction algorithm such as LLL on $\bar{B}_{c'(x,y)}$. Notice we can recover $4e'_{00} + m'$ as $\alpha + \lceil\frac{15n}{2}\rceil = 4e'_{00} + m'$. So, if we view $4e'_{00} + m'$ as an integer we can recover $m' \bmod 4$ because the largest possible value of $4e'_{00} + m'$ is $15n$ which is significantly less then q.

We can use this to break IND-CPA, by choosing m_1 and m_2 such that when viewed as integers, $m'_1 \bmod 4 \neq m'_2 \bmod 4$. Since, for any ciphertext that encrypts a message m, we can recover $m' \bmod 4$, we will be able to tell whether the Oracle encrypted m_1 or if the Oracle encrypted m_2. Notice that our attack obtains a distinguishing advantage of 1 and works independent of the size of q.

Finally, the fact that the extended lattice corresponding to $c'(x,y)$ has an unusually short vector is what allows us to distinguish ciphertexts from random degree 2 polynomials sampled uniformly from $R_q[x,y]$ because experimental evidence shows that if $g(x,y)$ is sampled uniformly from $R_q[x,y]$ then the LLL reduced basis of extended lattice that corresponds to $g'(x,y)$ will have much larger components. When we uniformly sampled $g(x,y)$ from $R_q[x,y]$ 1,000 times, 998 times $\mathrm{LLL}(\bar{B}_{g'(x,y)})$ did not contain a row where the last entry is 1 or -1 implying that $g(x,y)$ is not a ciphertext because the dimension of the lattice is only 7. Further when the $\mathrm{LLL}(\bar{B}_{g'(x,y)})$ contains a row where the last entry is 1 or -1 the average Euclidean norm of such a row is much larger than the average Euclidean norm of the shortest row of $\mathrm{LLL}(\bar{B}_{c'(x,y)})$ i.e. $[\vec{e}|1]$. On one hand, out of 100 sampled ciphertexts the average Euclidean norm of the the shortest row corresponding to actual an ciphertext is about $531.212 \approx 2^{9.053}$. While on the other hand, out of 100 sampled $\mathrm{LLL}(\bar{B}_{g'(x,y)})$ the other average Euclidean norm was about $10090.175 \approx 2^{13.301}$.

References

[1] K. Akiyama, Y. Goto, S. Okumura, T. Takagi, K. Nuida, G. Hanaoka, H. Shimizu and Y. Ikematsu, A public-key encryption scheme based on non-linear indeterminate equations (giophantus), *Cryptology ePrint Archive, Report 2017/1241*, (2017). Available from: https://eprint.iacr.org/2017/1241.

[2] K. Akiyama, Indeterminate equation public-key cryptosystem "*Giophantus*", *First PQC Standardization Conference*, Fort Lauderdale FL. USA, (2018). Available from: https://csrc.nist.gov/CSRC/media/Presentations/Giophantus/images-media/Giophantus-April2018.pdf.

[3] M. R. Albrecht, R. Fitzpatrick and F. Göpfert, On the efficacy of solving LWE by reduction to unique-SVP, *Information Security and Cryptology – ICISC*, (2013), 293–310. Available from: https://eprint.iacr.org/2013/602.

[4] W. Beullens, W. Castryck and F. Vercauteren, IND-CPA attack on Giophantus, (2018), Available from: https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/round-1/official-comments/Giophantus-official-comment.pdf.

[5] J. T. Ding, S. Alsayigh, R. V. Saraswathy, S. Fluhrer and X. D. Lin, Leakage of Signal function with reused keys in RLWE key exchange, *2017 IEEE International Conference on Communications (ICC)*, (2017). Available from: https://eprint.iacr.org/2016/1176.

[6] S. Fluhrer, Cryptanalysis of ring-LWE based key exchange with key share reuse, 2016, Available from: https://eprint.iacr.org/2016/085.

[7] P. Nguyen, Giophantus and *LWR-based submissions, 2018, Available from: https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/round-1/official-comments/Giophantus-official-comment.pdf.

[8] O. Regev, On lattices, learning with errors, random linear codes, and cryptography, *STOC'05: Proceedings of the Annual ACM Symposium on Theory of Computing*, (2005), 84–93.

Received February 2019; revised March 2019.

E-mail address: jintai.ding@gmail.com
E-mail address: deatonju@mail.uc.edu
E-mail address: schmidku@mail.uc.edu